POLICY PAPER

Building Resilience against Digitally-Enabled Scams in ASEAN

October 2025

TECH FOR GOOD INSTITUTE

TABLE OF CONTENTS

About This Paper 2

Executive Summary 8

I. An Urgent Issue for ASEAN: Digitally-Enabled Scams 13

A. ASEAN Digital Safety Foundations 14

B. Building on this Foundation: Tackling Scams across ASEAN 16

1. Technology and Data 17

2. People 18

3. Institutions and Coordination 18

4. Policy 19

II. Building Regional Resilience against Scams 20

A. Supporting National Capacity 20

1. Facilitating knowledge exchange 20

2. Setting regional standards, protocols or principles for interoperability 21

3. Developing resources and toolkits 22

4. Facilitating technical assistance 23

B. Enabling Regional Collaboration 24

1. Strengthening Regional Identity Verification and Reducing Anonymity 24

2. Advancing Intelligence Sharing and Data Interoperability 24

3. Regional Cooperation for Response and Recovery 25

4. Collaborative Innovation 26

III. A Whole-of-ASEAN Approach against Scams 28

References 30

About This Paper

This paper is the output of the Digital Working Group 2025 of the ASEAN Think Tank Summit (ATTS), an ASEAN-ISIS initiative coordinated by the Singapore Institute of International Affairs and supported by the ASEAN Secretariat. The ATTS aims to revitalise Track 2 level discussions by generating ideas for ASEAN's development and providing policy inputs into the ASEAN process.

This paper builds on the Tech for Good Institute's paper *Building Resilience Against Scams and Fraud across Southeast Asia-6 (SEA-6)*, focusing on the need for cooperation amongst ASEAN Member States (AMS) to tackle the challenge of digitally-enabled scams. In particular, this paper explores the role ASEAN may play in facilitating this concerted effort that spans the political-security, economic and socio-cultural communities within the association. These urgent areas for cooperation include aligning SIM registration and digital identity standards, harmonising scam definitions and reporting protocols, establishing intelligence-sharing mechanisms, coordinating enforcement and victim support, and developing interoperable technologies and regional training frameworks.

This paper comprises the inputs of over 100 participants from Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, the Philippines, Singapore, Thailand and Vietnam from across the public, private and civil sectors. The findings are aligned with the Bangkok Digital Declaration, adopted by ASEAN Digital Ministers in January 2025, which calls for coordinated scam prevention, cross-border enforcement, and partnerships with financial institutions and digital platforms.[1]

This version of the paper will be presented and deliberated at the 2025 ATTS, and subsequently submitted to ASEAN Sectoral Bodies, the Committee of Permanent Representatives to ASEAN, and the relevant Senior Official Meeting (SOM) of AMS, and the ASEAN Secretariat for consideration. This paper offers a starting point for continued dialogue among ASEAN sectoral bodies, the Secretariat, Senior Officials, and national governments. Grounded in regional realities, its ideas are intended to evolve through feedback and collaboration.

Acknowledgements

Special thanks to the Singapore Institute of International Affairs (SIIA) for convening the ATTS. We are also indebted to the members of the Digital Working Group for their active engagement and feedback that made this policy paper possible. Their inputs were central to shaping the findings and recommendations of this regional report.

- AI Forum
- Alliance of Tech Innovators for the Nation
- Asian Development Bank
- Asia Program at Carnegie Endowment for International Peace
- Bamboo Builders
- Cambodian Institute for Cooperation & Peace
- Centre for Strategic and International Studies
- Department of Information and Communications Technology, Philippines
- Global Anti-Scam Alliance
- Google
- HSBC
- Institute of Strategic & International Studies (ISIS) Malaysia
- ISEAS - Yusof Ishak Institute
- Lee Kuan Yew School of Public Policy, National University of Singapore
- Ministry of Digital, Malaysia
- Ministry of Industry and Commerce, Lao DPR
- Phenikaa University Vietnam
- The Institute of Strategic & International Studies (ISIS) Thailand
- The National Tech Association of Malaysia (PIKOM)
- Royal Melbourne Institute of Technology (RMIT) Vietnam
- School of Criminology & Criminal Justice, Griffith University
- Singapore Institute of International Affairs
- Thailand Consumers Council
- TikTok

This paper also builds on and incorporates insights from participants who provided national level insights, some as part of a SEA-6 study, *Building Resilience against Scams and Fraud across Southeast Asia,* supported by Google.org and Bamboo Builders. The Institute is grateful to Google.org and Bamboo Builders for supporting foundational conversations that included ministries, regulators, financial institutions, digital platforms, think tanks, and consumer groups across the region:

Brunei	Cambodia
● University of Brunei Darussalam ● Authority of Info-communications and Technology Industry of Brunei Darussalam (AITI)	● Cambodian Institute for Cooperation & Peace (CICP) ● Italian Business Chamber of Cambodia ● Youth Council of Cambodia ● CORD Global ● Cambodian Institute for Cooperation & Peace (CICP) ● AI Forum
Indonesia	**Lao PDR**
● Coordinating Ministry for Economic Affairs (Kemenko Perekonomian) ● Ministry of Trade (Kemendag) ● Ministry of Communications and Digital Affairs (Komdigi) ● National Consumer Protection Agency (BPKN) ● Financial Services Authority (OJK) ● Indonesian Chamber of Commerce (KADIN) ● Indonesia Cyber Security and Digitalisation Association (ADIGSI) ● Centre for Strategic and International Studies ● Center for Indonesian Policy Studies ● Southeast Asia Freedom of Expression Network (SAFEnet) ● Center for Digital Society ● Indonesia Services Dialogue Council	● Ministry of Industry and Commerce ● Institute of Foreign Affairs, Lao PDR ● LaoCERT
Malaysia	**Philippines**
● Cybersecurity Malaysia ● Malaysia Digital Economy Corporation (MDEC) ● MyDigital ● CelcomDigi ● AEON Bank Malaysia ● Institute of Strategic and International Studies	● Bangko Sentral ng Pilipinas ● Senate of the Philippines ● Department of Information and Communications Technology (DICT) ● Analytics and Artificial Intelligence Association of the Philippines ● Better Than Cash Alliance

● Malaysia Crime Prevention Foundation ● Universiti Malaya ● Multimedia University ● Universiti Tunku Abdul Rahman	● Bankers Association of the Philippines ● Credit Card Association of the Philippines ● Globe Telecom ● BDO Unibank ● Rizal Commercial Banking Corporation (RCBC) ● Global Forum on Cyber Expertise (GFCE) ● Asian Institute of Management (AIM) ● Scamwatch Pilipinas and Truth 360
Singapore	**Thailand**
● Ministry of Home Affairs (MHA) ● GovTech Singapore ● GSMA ● OCBC Bank ● Rajah & Tann Technologies ● ST Engineering ● Association of Certified Anti-Money Laundering Specialists ● Hong Leong Finance ● Bamboo Builders ● NTU Digital Trust Centre (DTC) ● Lee Kuan Yew School of Public Policy ● S. Rajaratnam School of International Studies (RSIS)	● Bank of Thailand (BOT) ● Electronic Transactions Development Agency (ETDA) ● Foundation for Consumers (FCC) ● Thailand Consumers Council (TCC) ● Collaborative Fact Checking (COFACT) Thailand ● Thammasat University
Vietnam	**Other Participants (Multiple Countries)**
● Central Committee for Policy and Strategy ● Pacific Links Foundation ● FPT Information System ● RMIT University Vietnam ● Institute for Policy Studies and Media Development (IPS) ● Vietnam Academy of Social Sciences ● Vietnam National University	● Amazon ● Feedzai ● Google ● Gogolook ● Mastercard

*Note: *Some organisations have requested to remain anonymous.*

Finally, TFGI's role in the DWG and this paper would also not have been possible without Grab's support for TFGI's mission of leveraging the promise of technology and the digital economy for inclusive, equitable and sustainable growth across the region.

About TFGI

The Tech for Good Institute is a non-profit organisation working to advance the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia (SEA). With a population twice the size of the US and strong demographics, SEA's digital economy is evolving rapidly. At the same time, the region's trajectory is unique, shaped by its diverse cultural, social, political and economic contexts. The Tech for Good Institute serves as a platform for research, conversations and collaborations focused on SEA, while staying connected to the rest of the world. Our work is centred on issues at the intersection of technology, society and the economy, and is intrinsically linked to the region's development. We seek to understand and inform policy with rigour, balance and perspective by using research, effective outreach and evidence-based recommendations.

The Institute was founded by Grab, to advance the vision of a thriving and innovative SEA for all. We welcome opportunities for partnership and support, financial or in-kind, from organisations and individuals committed to fostering responsible innovation and digital progress for sustainable growth in the region.

Funders do not determine research findings nor the insights and recommendations of research.

More information about the Institute can be accessed at www.techforgoodinstitute.org.

About SIIA

The Singapore Institute of International Affairs (SIIA) provides insights and perspectives for policymakers, businesses and individuals in navigating issues facing the world. Our work serves as a bridge between these stakeholders, to nudge policy change through dialogue and collective action.

As a founding member of the ASEAN-ISIS (ASEAN Institutes of Strategic and International Studies) network since 1988, SIIA engages in Track 2 diplomacy, fostering dialogue among stakeholders in our region and beyond.

SIIA has been consistently ranked as one of the leading think tanks in SEA and the Pacific, in the Global Go-To Think Tank Index* by the University of Pennsylvania. Since 2017, SIIA has ranked the No. 1 independent think tank in Asia. SIIA is also recognised as one of the top 50 think tanks globally, excluding the United States of America. In 2019, SIIA was recognised as the No. 1 think tank in South Asia, SEA, and the Pacific (excluding India). In 2020, SIIA was also recognised as one of the think tanks with the best policy and institutional response to the COVID-19 pandemic.

About ASEAN-ISIS Network

The Asean-ISIS Network is an association of think-tanks registered with ASEAN. Formed in 1988, its founding members comprise the Centre for Strategic and International Studies (CSIS) of Indonesia, Institute of Strategic and International Studies (ISIS) Malaysia, Institute of Strategic and Development Studies (ISDS Philippines), Singapore Institute of International Affairs (SIIA), and Institute of Security and International Studies (ISIS) of Thailand. The network also includes the Brunei Darussalam Institute of Policy and Strategic Studies (BDIPSS), Cambodian Institute for Cooperation and Peace (CICP), Diplomatic Academy of Vietnam (DAV), Institute of Foreign Affairs (IFA) of the Lao People's Democratic Republic and Myanmar Institute of Strategic and International Studies (MISIS).

The network encourages cooperation among scholars and analysts and promotes policy-oriented studies and exchanges of information on issues affecting SEA's peace and security. It also serves as a platform for Track 2 diplomacy and enjoys a close relationship with AMS.

Disclaimer

The information in this paper is provided on an "as is" basis. This paper is not to be considered as a recommendation for investments in any industry. This document is produced by the Tech for Good Institute and has been prepared solely for information purposes over a limited time period to provide a perspective on the region. The Institute and any of its affiliates, or any third party involved make no representation or warranty, either expressed or implied, as to the accuracy or completeness of the information in the paper, and no responsibility or liability whatsoever is accepted by any person of the Institute, its affiliates and its respective officers, employees or agents.

Copyright © 2025 by the Tech for Good Institute. All rights reserved.

Permission is granted for reproduction of this file or its contents, with attribution to the Tech for Good Institute.

Executive Summary

Digitally-enabled scams have been responsible for an estimated US$688.42 billion financial losses in 2024 and emerged as an urgent, transnational threat to the digital ecosystem. According to the Global Anti-Scam Alliance, more than half of global scam-related losses originate in Asia. Scams span online and offline domains, exploit both technical and behavioural vulnerabilities, and cut across sectors and borders. They are growing in scale, speed and sophistication, requiring a multi-disciplinary, multi-sectoral and multi-stakeholder response at domestic, regional and global levels.

Since 2017, ASEAN has advanced regional cybersecurity through initiatives such as the ASEAN Cybersecurity Cooperation Strategy and more recently the ASEAN Computer Emergency Response Team (CERT). Scam management requires similar national capacity and cross-border cooperation, with a cross-sectoral ecosystem approach. Recommendations are therefore structured around supporting the national capacity of ASEAN Member States (AMS) and strengthening regional coordination and cooperation through ASEAN.

Supporting National Capacity

Domestic resilience to scams encompasses prevention, detection, response and adaptation across the digital ecosystem, including but not limited to finance, telecommunications and digital platforms. Scams exploit both technical and behavioural vulnerabilities. Resilience must therefore be built through multisectoral action that combines technology, people, institutions, regulation, and processes. ASEAN can support AMS in strengthening their national readiness along the following dimensions:

- **Technology**: Robust and interoperable digital infrastructure is essential for detecting, preventing and disrupting scams. ASEAN could support AMS, for example, by advancing common standards and offering technical assistance for interoperability.

- **People:** Social interventions play a critical role in detecting scams early, changing risky behaviours and protecting vulnerable groups. Educators, civil society organisations, community leaders and media all play important roles in raising awareness, identifying threats and providing support. The ASEAN Socio-Cultural Community can help AMS mobilise trusted community figures through train-the-trainer programmes, practice sharing and toolkits to tackle scams through trusted community networks in culturally-relevant ways.

- **Institutions and coordination:** Given the multi-sectoral and multi-disciplinary nature of scam management, AMS could establish dedicated national anti-scam coordination units with clear mandates, resources and lines of accountability. These anti-scam units bring public agencies together for coordinated responses, such as integrating cybersecurity and law enforcement. These units can also facilitate partnership with the private and civil sectors. ASEAN can support AMS in implementing such inter-agency

coordination models by providing guidance notes, good practice templates and frameworks, and peer learning amongst AMS and ASEAN dialogue partners.

Workflows that span agencies, from education to law-enforcement, also require coordination. For example, treating individuals coerced into scam operations as victims rather than criminals can encourage more people to come forward with information. ASEAN can add value by promoting shared practice, for example supporting the implementation of the non-punishment principle, already endorsed by ASEAN, and developing practical guidance to help AMS to embed victim-sensitive protocols within national law enforcement systems.

- **Policy**: Clear, coherent, and up-to-date legal frameworks are essential for closing loopholes and addressing fragmented mandates that scammers exploit. ASEAN can support AMS in regulatory reform in areas such as payments, cybercrime and consumer protection, ensuring they are fit for the digital age.

In summary, ASEAN can support AMS readiness against scams through targeted frameworks, structured knowledge exchange and practical technical assistance, such as toolkits and training programmes. These efforts lay the foundation for deeper regional cooperation at the ASEAN and global levels.

Strengthening Regional Coordination and Cooperation

Strong national responses are essential but are not sufficient. Across SEA, every stage of the scam value chain is likely to cross borders. Perpetrators may operate from one country, the enabling infrastructure, such as payment systems, online platforms and SIM cards, may be based in another, and victims may reside in yet another AMS. No AMS can address the problem effectively alone, underscoring the need for coordinated action at both regional and global levels.

ASEAN, in particular through the ASEAN Working Group on Anti-Online Scams (WG-AS), can bring coherence, interoperability and mutual support across the region for the prevention, detection, response and adaptation to this evolving threat.

- **Awareness and Prevention**: Combine technical and procedural safeguards, such as aligning SIM registration and digital identity standards (*Technology*) and standardising caller verification protocols like STIR/SHAKEN and RCS Business Messaging (RBM) (*Processes)*, with best practice sharing on public awareness campaigns (*People*).

- **Identification and Detection**: Effective scam prevention depends on a shared understanding of the threat. Without common definitions and consistent reporting, intelligence remains fragmented. ASEAN can help close this gap by developing a unified regional scam taxonomy and a minimum reporting schema aligned with the ASEAN Data Management Framework, enabling AMS to speak the same “language”

when sharing information. Much like how the ASEAN CERT facilitates coordinated responses to cybersecurity incidents, a dedicated Scam Intelligence Exchange would allow AMS to pool insights in real time, detect emerging patterns, and act faster against cross-border scams.

- **Coordinate Response and Recovery**: Cross-border scams demand rapid, coordinated enforcement and victim support that no single AMS can deliver alone. ASEAN can strengthen this capacity by establishing a regional task force to conduct joint operations, test enforcement protocols, and embed victim assistance into regional frameworks. This mechanism could be hosted under an existing body, such as ASEANAPOL, or developed as a new dedicated structure to ensure operational readiness across the region.

- **Foster Adaptation through Innovation:** Building on the Technology pillar of national capacity, ASEAN can help AMS stay ahead of fast-evolving scam tactics by identifying and promoting a set of interoperable technology solutions, AI-enabled or otherwise, that can detect scams, automate responses, and analyse emerging threats. This could include developing shared technical standards, creating sandbox corridors to pilot and evaluate solutions simultaneously across AMS, and using approaches like federated learning to enable secure, cross-border data use without compromising privacy. By doing so, less-mature AMS can benefit from proven tools, while more advanced AMS can set global benchmarks for interoperable, high-impact anti-scam solutions.

ASEAN can take a pragmatic approach by coordinating and strengthening existing structures rather than creating new ones. Given the resources and mandate, the Working Group on Anti-Scams (WG-AS) could convene sectoral bodies already advancing anti-scam efforts. These include ADGMIN and ADGSOM on technology standards and interoperability, the Working Group on Trafficking in Persons on exploitation in scam centres, Working Committee on Payment and Settlement Systems (WC-PSS) on securing cross-border payments, and ASEANAPOL on joint enforcement and intelligence-sharing. On the economic side, ASEAN Economic Ministers (AEM), supported by the Senior Economic Officials Meeting (SEOM) and WC-ECOM (WC-ECOM), can support the online safety provisions of the Digital Economy Framework Agreement (DEFA), once concluded.

A modular approach can accommodate the diversity of national approaches reflecting the range AMS' prioritisation and capacity for intervention. Mechanisms like ASEAN Minus X allow willing AMS to move ahead while others join later, maintaining momentum without requiring full consensus. Meanwhile, DEFA could provide additional momentum for alignment as scam management is a core safety and resilience imperative for an inclusive, and interoperable digital future for the region. ASEAN's role in coordinating action within and across borders can strengthen collective defences, protect citizens, and foster trust in the digital economy, with the potential to demonstrate how our region may evolve from a scam hotspot to an example of a multi-stakeholder approach to scam resilience.

TECH FOR GOOD INSTITUTE

Glossary

Term	Definition
ACID	ASEAN Computer Emergency Response Team Incident Drill, an annual exercise to test and strengthen regional incident response capabilities.
ADGMIN	ASEAN Digital Ministers' Meeting setting regional digital policies.
ADM2025	ASEAN Digital Masterplan 2025, outlining regional priorities for trusted digital services, digital literacy, and a secure, inclusive digital ecosystem.
AJCCBC	ASEAN Japan Cybersecurity Capacity Building Centre for regional cyber training.
AMS	ASEAN Member States comprising the ten countries in the region (11 in October 2025 with Timor Leste).
ASCCE	ASEAN Singapore Cybersecurity Centre of Excellence for capacity-building.
ASCom	Singapore's Anti-Scam Command coordinating real-time scam responses.
ASEAN	Association of Southeast Asian Nations, the intergovernmental organisation established in 1967 to promote cooperation, integration, and stability among its Member States.
ASEAN CERT	Network of national Computer Emergency Response Teams across ASEAN.
ASEAN Mutual Legal Assistance Treaty	Legal framework for cross-border law enforcement cooperation.
ASEANAPOL	The ASEAN Chiefs of National Police coordinating regional law enforcement.
ASEAN-minus-X / 2+X Model	Flexible cooperation format allowing subsets of AMS to move ahead on initiatives.
ASEC	ASEAN Secretariat coordinating ASEAN's regional agenda.
Bali Process	Regional forum addressing human trafficking and transnational crime.
Bangkok Digital Declaration	Adopted in January 2025, committing ASEAN to secure, innovative, and inclusive digital cooperation, including actions to address scams.

Cyber SEA Game	Gamified ASEAN platform for cybersecurity skills training.
DEFA	ASEAN Digital Economy Framework Agreement
nTrust	Vietnam's scam-checking app using live databases.
RBM (RCS Business Messaging)	Verified messaging system to block spoofing.
ScamShield	Singapore's app that blocks scam calls and texts.
SEA	Southeast Asia, a geographical region encompassing the ten ASEAN Member States (AMS) and Timor-Leste, which will become a full ASEAN member in October 2025.
SOMTC	ASEAN Senior Officials Meeting on Transnational Crime.
STIR/SHAKEN	Protocol to verify caller IDs and stop call spoofing.
WG-AS	ASEAN Working Group on Anti-Online Scam, coordinating preventive, enforcement, and awareness-raising measures against online scams across AMS.

I. An Urgent Issue for ASEAN: Digitally-Enabled Scams

The Kuala Lumpur Declaration on ASEAN 2045 called for an ASEAN that is "resilient, innovative, dynamic and people-centred," with a region that is connected through an open, secure, and trusted digital ecosystem. This forward-looking vision reflects a Southeast Asia (SEA) that embraces digital transformation on a foundation of digital trust, actively safeguarding its people, institutions, and economies from emerging risks.

In this context, building a safe and trustworthy digital environment is central to ASEAN's long-term competitiveness, inclusion and regional integration. Digital resilience, the ability to withstand, adapt to, and recover from digital disruptions while maintaining essential functions and evolving to address future risks, is critical to realising this vision.

SEA's rapid digital transformation means that governments, businesses, and citizens increasingly depend on digital technologies for commerce, governance, education, and daily life. The pace and scale of adoption have been accompanied by rapid growth of digitally-enabled crimes and harms, ranging from cyberattacks and data breaches to misinformation, online harassment and scams. These threats have grown into systemic risks with transnational reach.

In the case of online and digitally-enabled scams, the threat landscape is fast-evolving in both scale and sophistication. In 2023 alone, such operations were estimated to have generated over USD 37 billion in losses globally.[2] Like cyber-attacks, scams are globalised and industrialised operations. **Asia accounts for more than half of the world's scam-related losses, according to the Global Anti-Scam Alliance.**[3] Hence, SEA needs a coherent regional approach to digital scam prevention, and ASEAN is well-placed to support the development and execution of this endeavour.

A. ASEAN Digital Safety Foundations

Over the last decade, ASEAN has prioritised digital transformation and integration to foster a seamless, connected digital economy across AMS. This commitment is reflected in frameworks such as the ASEAN Digital Masterplan 2025[4], which sets out objectives like enhancing trusted digital services, promoting digital literacy, and fostering a secure, inclusive ecosystem.

Cybersecurity has been central to this digital agenda. The ASEAN Cybersecurity Cooperation Strategy, initially launched in 2017 and updated in 2022, formalised regional cooperation in incident response, CERT coordination, and capacity building. In 2024, AMS signed the legally-binding ASEAN CERT Framework reinforcing mechanisms for cross-border threat intelligence, joint training, and coordinated response. Efforts to operationalise a physical ASEAN Regional CERT, hosted in Singapore, further cemented this evolution. The ASEAN Cybersecurity Capacity Building Programme, also established in 2024, provided a platform for best practice and expertise sharing, and an avenue for accessing training and technical assistance.

From Cybersecurity to Digital Safety

Recent ASEAN initiatives show a shift from a technical cybersecurity lens toward a broader digital safety agenda to go beyond preventing cyberattacks to protecting citizens from data breaches and scams (Table 1). The forthcoming ASEAN Digital Economy Framework Agreement (DEFA) explicitly distinguishes digital safety from cybersecurity to build an interoperable, open and trusted digital ecosystem. Digital safety encompasses a broad range of issues, including scams, harmful content, protection of vulnerable groups such as children, and online harassment. Many areas of digital safety, including scams, are unlike traditional cyber threats, in that technical vulnerabilities are only one avenue of attack. Scammers also exploit human behaviour, legal loopholes, and fragmented enforcement.

Table 1: From Cybersecurity to Digital Safety in ASEAN

ASEAN Initiative	Year	Cybersecurity	Data Protection	Scams
ASEAN Cybersecurity Cooperation Strategy	2017, 2022 update	✓		
ASEAN Digital Integration Framework	2018	✓	✓	
ASEAN Regional Computer Emergency Response Team (ASEAN-CERT)	2018	✓		
ASEAN Computer Emergency Response Team Incident Drill (ACID)	2018	✓		
ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)	2018	✓		
ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)	2019	✓		
ASEAN Digital Masterplan 2025 (ADM2025)	2021	✓	✓	
ASEAN Digital Economy Framework Agreement (DEFA) *(under development)*	2023-2025		✓	✓
Bangkok Digital Declaration	2025	✓	✓	✓
ASEAN Working Group on Anti-Online Scam (WG-AS)	2025			✓
ASEAN Guideline on the Non-Punishment Principle (for trafficked scam victims)	2025			✓

Note: List not Exhaustive

B. Building on this Foundation: Tackling Scams across ASEAN

AMS' commitment to tackling scams was formalised in the Bangkok Declaration on Combating Online Scams in January 2025,[5] setting out regional priorities for prevention, victim protection, and cross-border cooperation. Such an all-of-ASEAN approach is needed across the association's political-security, economic, and socio-cultural pillars given the complexity of the scam economy. The scam economy comprises industrialised, dynamic operations spanning multiple sectors including telecommunications providers, financial institutions, digital platforms, logistics operators, and offline actors in both formal and informal economies.

The complexity of this challenge is reflected in the establishment of the ASEAN Working Group on Anti-Online Scams (WG-AS) at the 4th ASEAN Digital Ministers' Meeting (ADGMIN) in February 2024, and the first ASEANAPOL Working Group Meeting on Anti-Scam Operations, hosted by the ASEANAPOL Secretariat in March 2025. WG-AS brings together law enforcement, telecom regulators, consumer protection agencies, and digital economy officials to coordinate preventive, enforcement, and awareness-raising measures, while the ASEANAPOL Working Group focuses on joint enforcement and intelligence-sharing on eliminating scam centres in particular. ASEAN has facilitated collaboration between the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) and the ASEAN Intergovernmental Commission on Human Rights (AICHR) to launch a guideline on the non-punishment principle for individuals trafficked into scam operations in June 2025.[6] This guideline calls on AMS to ensure victims coerced into scams are protected and not criminalised, embedding victim-sensitive approaches into national law enforcement protocols.

Looking ahead, scam management requires investments and action across four dimensions: *(i) Technology and Data, (ii) People, (iii)) Institutions* and *Coordination*, and (iv) *Policy:*

- **Technology and Data** involve the infrastructure, tools, and protocols for detection, prevention, and disruption. Secure sharing and interoperability across these data from public and private stakeholders, including but not limited to telecom operators, payment providers, and platform companies, are essential for proactive security, response, and innovation.
- **People** cover trusted community figures, public awareness actors, and frontline responders such as educators, community leaders, police officers, and bank staff.
- **Institutions and Coordination** refer to government agencies, regulators, and national bodies responsible for aligning efforts across sectors and streamlining responses.
- **Policy** is a comprehensive effort setting the legal and regulatory framework, closing loopholes, embedding victim protection and enabling innovation.

1. *Technology and Data*

As scammers exploit technologies to scale their attacks at scale, AMS need to respond with equally adaptive and innovative technologies.

For example, secure and inclusive digital identity and authentication in the form of digital public infrastructure enables robust identity verification and reduces anonymity for bad actors. Advanced authentication protocols, including STIR/SHAKEN for caller ID authentication[7] and RCS Business Messaging (RBM) for verifying legitimate business communications,[8] are also technological solutions that can detect, and block spoofed or fraudulent communications before they reach users.

For detection, federated learning models offer a privacy-preserving way for telecommunications providers to collaboratively train machine learning systems to spot scam patterns. By improving anomaly detection—such as phishing or spoofing attempts—without exposing raw user data, such technologies can support national data management and data protection policies.

Data itself is a crucial enabler. The patterns embedded in telecommunications traffic, payment flows, and platform activity often present the first indications of an emerging scam. Today, however, these insights remain siloed across operators, financial institutions, and digital platforms. Secure modalities for sharing and interoperability are thus critical. Without common standards, threats will manoeuvre through institutional and jurisdictional gaps. ASEAN can add value by developing trusted frameworks that allow stakeholders to collectively contribute, access, and act on intelligence.

Artificial intelligence (AI) also holds much potential in enhancing detection, triage and recovery, enabling faster identification of emerging threats, better prioritisation of cases and more efficient victim recovery workflows. In the United Kingdom for example, Mastercard has partnered with nine UK banks to use AI-powered insights and large-scale payments data to predict and block scam payments in real time before funds leave a victim's account.[9] Building on five years of collaboration tracing mule accounts, the solution overlays transaction patterns and risk indicators with AI analysis to give banks the intelligence needed to intervene and stop scams across multiple payment types. Similar innovations are also emerging in SEA. For instance, Singtel, AIS (Thailand), and Maxis (Malaysia) recently partnered to jointly combat rising cross-border digital scams, signalling how regional operators are beginning to pool intelligence and explore AI-enabled approaches to scam detection and prevention.[10]

Another application of generative AI is in the use of AI bots, where technology providers and telecommunications companies can divert suspicious calls or messages to automated systems. These bots can both gather intelligence and waste scammers' time, reducing their capacity to target real victims.

2. *People*

Community engagement is essential to raise awareness of scams, especially in areas with low digital literacy or limited institutional trust. In addition to national-level public awareness campaigns, trusted figures such as religious leaders, youth advocates, and local influencers can develop and deliver culturally relevant and locally resonant messaging. These individuals can amplify formal campaigns and adapt content to reflect community-specific needs and contexts.

Equipping frontline responders, such as police officers, bank staff and telecommunication provider representatives, can also support scam mitigation. Scam victims often endure more than just financial loss. Many also face psychological trauma, emotional distress, shame and social stigma, most notable in romance scams.[11] In Thailand, for instance, 73% of scam victims reported experiencing a strong emotional toll.[12] In Malaysia, 63% of victims noted a significant decline in trust toward digital platforms following scam incidents.[13] Moreover, when stolen identities are used in further fraudulent activities, victims may suffer reputational harm, compounding the long-term impact.[14]

Structured training programmes for frontline responders to support scam victims with empathy, clarity and up-to-date knowledge, can remove stigma, encourage help-seeking behaviour and improve reporting rates. A potential model is Singapore's ScamShield Victim Care Officers (VCOs), who are trained to provide both emotional and practical support to scam victims navigating the criminal justice process.[15] VCOs also guide victims toward relevant community services that address trauma and distress. Curricula should cover trauma-informed communication, multilingual service delivery, culturally inclusive practices, and practical guidance on scam reporting, recovery, and mental health referrals.

3. *Institutions and Coordination*

Prevention, detection and management require inter-agency coordination within government, such as amongst different agencies, law enforcement, financial regulators, telecommunications authorities,[16] as well as with the private sector.

National Anti-Scam Coordination Units can bridge the multi-dimensional and multi-sectoral nature of scam management by centralising and strengthening domestic responses. These units can be operationalised by embedding national anti-scam centres within existing cybersecurity infrastructure, such as Computer Emergency Response Teams (CERTs). Partnership with public and private stakeholders, including law enforcement agencies, financial institutions, telecommunications providers, and digital platforms streamlines coordination and significantly enhances response capabilities.

Such centres would be well-positioned to engage in real-time threat monitoring, participate in regional training initiatives, and facilitate secure information sharing on emerging risks. Malaysia's National Scam Response Centre (NSRC), established in October 2022, illustrates

this approach. Bringing together Bank Negara Malaysia, the Royal Malaysia Police, the Malaysian Communications and Multimedia Commission, and the National Anti-Financial Crime Centre, the NSRC provides a single 24/7 channel for victims to report scams, enabling faster action such as alerting banks to block fraudulent transactions, coordinating with telecom providers, and issuing public advisories. To support these efforts, ASEAN can help by documenting case studies like NSRC, providing guidance on institutional setup and offering shared training modules to strengthen national units.

4. Policy

Clear, coherent, and up-to-date legal frameworks are essential for closing loopholes and addressing fragmented mandates that scammers exploit. Definitions of fraud, payments acts, cybercrime provisions, consumer protection statutes and responsibility-sharing arrangement, to name a few, might need to be reviewed.

An example of supportive policy for scam management is the non-punishment principle for individuals coerced or trafficked into scam operations. Ensuring that these individuals are treated as victims rather than criminals[17] is vital for fostering trust between communities and law enforcement agencies. When victims can report scams without fear of prosecution, they are more likely to come forward, enabling authorities to target investigative efforts toward genuine perpetrators. Embedding this principle in national law enforcement protocols involves training frontline officers, prosecutors, and judicial officials to recognise coerced victims, understand relevant criteria, and apply guidelines consistently across enforcement, immigration and financial crime units.

In addition, AMS could strengthen their domestic policy capacity by establishing a clear taxonomy and typology of scam offences in national legislation to prevent gaps between cybercrime, financial fraud, and consumer protection laws. Payments and financial services regulations should also be updated to clarify the obligations of banks, fintech companies, telecom operators, and platforms in fraud monitoring, reporting, and redress. Laws should further mandate victim protection by requiring reporting channels, minimum standards for financial restitution, and access to psychological and legal support.

Furthermore, agile legislative review mechanisms, such as regulatory sandboxes or cross-government working groups, can foster an enabling environment for innovation to advance digital safety. technologies.

Strengthening institutional readiness is an enabler of regional and global resilience. Because scams are transnational, national efforts alone are insufficient. Interoperability, alignment and strong public–private partnerships are needed to counter the transnational effort of scammers, from consistent victim protection to data sharing across jurisdictions for coordinated protection and response, to encouraging scale for effective new solutions. . These foundations position ASEAN to drive regional cooperation and contribute to global responses against scams.

TECH FOR GOOD INSTITUTE

II. Building Regional Resilience against Scams

ASEAN's role in this evolving landscape is twofold. As a grouping, ASEAN can galvanise support for **National Capacity** while enabling **Regional Coordination** by serving as a platform for cooperation.

A. Supporting National Capacity

While national capacity forms the foundation of any effective response to scams, ASEAN has a unique opportunity to support AMS' readiness through:

1. facilitating knowledge exchange through documenting and sharing best practice/peer learning,
2. setting regional standards, protocols or principles for interoperability,
3. developing resources and toolkits, and
4. facilitating technical assistance.

Each of the domestic enablers, technology, people, institutions, and policy, may be enhanced through these ASEAN-level support mechanisms and primed for interoperability. Practical examples raised by the ATTS Digital Working Group for consideration include:

1. Facilitating knowledge exchange

- Technology and Data: **Create a regional knowledge and learning hub to consolidate resources** that support scam response and digital resilience. This platform could host toolkits, case studies, evaluation frameworks, after-action reports from simulation drills, and documented success stories from national initiatives. Inspired by models such as the World Economic Forum's Cybersecurity Learning Hub, it would serve as a dynamic, living repository.[18] Private sector actors could contribute tools, while non-profit organisations and community groups could share impactful grassroots initiatives, ensuring AMS at different stages of digital maturity have equitable access to high-quality resources.

  Several AMS have begun establishing digital identity regimes, they are at varying stages of implementation. Integration with telecommunications infrastructure also differs significantly across the region. Syndicates continue to exploit weak SIM registration systems and regulatory gaps in messaging platforms to avoid detection. For instance, Thailand has introduced biometric SIM registration using facial and fingerprint authentication, which other countries have yet to integrate.[19] Singapore, for example, has tightened SIM card registration and limited the number of SIM cards per subscriber.[20] ASEAN can support AMS by consolidating and sharing these experiences in the hub, allowing countries to draw lessons, adapt good practices, and avoid duplication of effort.

- People: **Provide a platform for sharing best practice and peer learning in community mobilisation** around scam awareness and prevention. While AMS are advancing public awareness efforts, these campaigns are typically designed in silos. An ASEAN Community Awareness Network could support cross-country coordination on scam prevention messaging and community-led outreach, host collaborative campaigns, align messaging with evolving scam typologies, and tailor public education to different demographic groups. ASEAN could also partner with multinational companies—especially in telecoms, finance, e-commerce, and digital platforms—to amplify anti-scam messaging across diverse channels.

- Institutions and coordination: **Establish a regional training framework for scam detection and response**, targeted at law enforcement agencies, financial regulators, platform operators, and CERTs. This framework should cover capabilities such as investigation techniques, digital forensics, public awareness campaign design, and multi-agency collaboration protocols. Regional institutions like the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)[21] and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)[22] are well placed to anchor this initiative. These centres could also host public-private simulation exercises, building on existing models like the Cyber SEA Game, which uses gamified scenarios to train professionals.[23]

- Policy: **Curate a repository of community engagement models to support policy implementation.** Awareness strategies benefit from partnerships amongst governments, the private sector, community organisations, educators, and grassroots leaders. Examples such as Malaysia's CelcomDigi programme and Singapore's ScamWise can provide scalable, culturally grounded models. Documenting these approaches as part of ASEAN's knowledge base can inform AMS's engagement strategies in ways that are relevant, responsive to evolving scam typologies and aligned to broader national policy objectives.

2. Setting regional standards, protocols or principles for interoperability

- Technology and Data: **ASEAN can promote interoperability of national digital identity systems** and **facilitate alignment of SIM registration systems** to enable cross-border verification. These measures will reduce anonymity, strengthen authentication, and provide a more secure digital ecosystem for AMS.

  ASEAN can also standardise verification protocols such as STIR/SHAKEN for caller authentication and RCS Business Messaging (RBM) for business communication could be rolled out consistently across AMS. These people-facing measures increase trust in communications, helping vulnerable users avoid scams.

- Institutions and coordination: **ASEAN could develop a shared regional scam taxonomy**. At present, AMS classify scams differently—investment fraud may be treated as cybercrime in one jurisdiction but financial fraud in another, while phishing definitions vary between email-only or multi-channel. A harmonised taxonomy, inspired by the ASEAN Taxonomy for Sustainable Finance, would improve data comparability, strengthen cooperation, and allow coordinated interventions across institutions.

- Policy: **Agreement on minimum reporting requirements and regional data standards** would support cross-border interoperability. Establishing clear protocols on how data should be collected, stored, and shared would ensure legal compatibility across AMS and reduce barriers to intelligence-sharing

3. Developing resources and toolkits

- Technology and Data: **ASEAN could coordinate the development of a regional catalogue of verified anti-scam tools.** This includes scam databases, AI-powered fraud detection systems, identity verification platforms, kill switches, and user-facing reporting applications. For example, Singapore's ScamShield, a government-developed app that blocks scam calls and texts, enables user reporting, and has recorded over 950,000 downloads, blocking 80,000 scam numbers and filtering more than 180 million messages.[24] Similarly, Vietnam's nTrust app allows users to verify phone numbers, QR codes, and accounts against a live fraud database of over one million flagged entries, contributing to a national scam intelligence network.[25] This regional catalogue should be overseen by a multi-stakeholder advisory group comprising technology providers, enforcement agencies, telecom operators, and civil society representatives. It would help AMS, particularly those with limited resources, adopt and adapt proven tools efficiently while ensuring alignment with regional priorities.

- People: ASEAN could **develop a regionally endorsed victim support training programme for frontline responders.** This programme should be delivered through ASEAN capacity-building platforms, and target key frontline actors such as law enforcement officers, immigration officers, hotline agents, social workers, and community advocates. Its goal is to embed a human-centric approach into digital resilience strategies across the region, especially when victims require cross-border support. Training modules should include gender and cultural sensitivity to ensure that vulnerable groups are not further marginalised during the response process.[26]

- Institutions and Coordination: ASEAN could **document potential models for inter-agency coordination and develop a practical toolkit for national anti-scam coordination units.** These coordinating units consolidate law enforcement, telecommunications regulators, financial authorities, and digital platforms under a single operational structure to enable a more effective and coordinated scam response. Singapore's Anti-Scam Command

(ASCom) offers a strong model. Operated by the Singapore Police Force, ASCom runs 24/7 and works closely with industry stakeholders such as banks, telecommunications providers and digital platforms to respond to reports. This allows the ASCom to freeze fraudulent accounts, disrupt scams in real-time, and expedite enforcement through standardised procedures.[27]

To support the operationalisation of the non-punishment principle, ASEAN can assist by **developing standardised training resources, hosting cross-border case workshops, and monitoring implementation** to promote consistency across AMS.

- Policy: **ASEAN can design model contractual clauses or guidance materials that will support AMS to integrate victim protection within a legal framework**. Examples could include minimum standards for financial compensation, complaint and resolution procedures, and access to psychological and legal support, all ensuring coherency for victim-centred responses.

4. Facilitating technical assistance

- Technology and Data: **ASEAN can serve as a channel to mobilise best-practice models and benchmarks** for fraud detection, identity verification, and intelligence-sharing protocols from dialogue partners, private sector actors, and development agencies. These technical resources would help AMS adopt effective practices in a timely manner, especially those with limited resources.

- People: **Through partnerships, ASEAN could convene the creation of a regionally accepted victim support training program for frontline responders** such as law enforcement, immigration officers, hotline and social workers, and community advocates. Such programs could be trauma-informed, gender-sensitive, and designed to equip responders for cross-border victim support.

- Institutions and Coordination: **ASEAN can reinforce existing capacity-building vehicles such as ASCCE or AJCCBC by integrating scam-specific training modules supported by external partners.** These could include investigation strategies, digital forensics, or protocols for multi-agency collaboration, complemented by joint simulation exercises. The ASEAN–Australia Counter Trafficking program's support in developing the guideline on the non-punishment principle provides a precedent for how technical assistance can be channelled effectively through ASEAN mechanisms.

- Policy: **ASEAN can act as a platform for sharing adaptable legislative models and regulatory mechanisms,** such as sandboxes that enable laws to adjust to new scam typologies or technologies. By documenting and disseminating practices for

information-sharing, escalation, and decision-making, ASEAN can provide AMS with reference points and benchmarks for refining their policies.

B. Enabling Regional Collaboration

In addition to national capacity, ASEAN is uniquely placed to promote cross-border cooperation and more integrated, proactive, and scalable approaches to tackling scams. Scams transcend borders, exploiting jurisdictional gaps, asynchronous regulations, and fragmented enforcement. No single country can tackle this alone. ASEAN can advance cooperation by embedding cross-border action across the four enablers. For example, urgent areas for cooperation at the technology and data level include digital identity, intelligence-sharing, and innovation, while effective response and recovery require people, institutions, and policy action. These areas can serve as practical starting points for collaboration, as they build on existing ASEAN mechanisms, are feasible for near-term implementation, and address critical gaps in regional scam management.

1. Strengthening Regional Identity Verification and Reducing Anonymity

Anonymity remains a key issue that makes scams harder to combat across the region. As highlighted in the national initiatives above, AMS are adopting diverse approaches to identity verification and SIM registration. These initiatives are currently country-specific and remain siloed. By embedding **unified verification standards in regional frameworks and implementation roadmaps**, ASEAN can adopt regionally harmonised requirements for digital identity authentication, SIM registration, and caller verification to reduce anonymity.

2. Advancing Intelligence Sharing and Data Interoperability

A foundational pillar of regional resilience is the ability to detect threats early, respond swiftly, and coordinate across jurisdictions. However, effective cross-border scam response depends on shared intelligence protocols and a common reporting language. Shared intelligence through common reporting protocols enables pattern detection, enforcement coordination and case escalation for collective digital resilience.

To enhance situational awareness and facilitate coordinated action, AMS can adopt a shared intelligence framework to move the region from siloed, reactive responses toward anticipatory, data-driven vigilance. In addition to the regional scam taxonomy, a standardised reporting schema aligned with the ASEAN Data Management Framework can support cross-border data exchange. The schema should specify required data fields, formats, and protocols for storage, preservation, and deletion.[28] A shared framework can form the basis for **an ASEAN Scam Intelligence Exchange.** With aligned data management and reporting, national-level initiatives could feed into a dedicated ASEAN Scam Intelligence Exchange to securely share key indicators of compromise, patterns, and threat signals. This would build situational awareness, enable early warning systems and support agile, data-driven enforcement. The Global Signal Exchange (GSE), developed by the DNS Research Federation, Google, and the Global Anti-

Scam Alliance, offers a useful model.[29] It connects digital economy companies such as Microsoft, Meta, telecoms, banks and security researchers to facilitate secure and near real-time exchange of phishing sites, scam content, and spoofed identities. Recently, Singapore's Govtech joined GSE to receive information about scam activity globally.

An ASEAN-specific exchange could complement global efforts by focusing on regional threats such as trafficking-linked scam centres and mule accounts, along ASEAN's data frameworks and scam taxonomy, and provide a trusted, regionally governed platform that addresses sovereignty concerns. Situating the platform within an AMS host could also build trust and cooperation. Importantly, it would also serve as a stepping stone to building the practice and processes around scam data collection and sharing, with partnerships with global platforms like GSE as a next step. In this way, ASEAN could act as both consolidator and partner to global efforts against scams, ensuring that the region's unique scam challenges are represented in global threat intelligence

To strengthen transparency and raise awareness, the Exchange could publish a regular *State of Scams in Southeast Asia* report to inform policymaking, guide platform and financial institution strategies, and support academic research. Over time, this could evolve into a public-facing dashboard visualising scam trends, affected sectors, financial impact, and response efforts, informing national, regional and global efforts to tackle scams.

Beyond cross-border knowledge exchange, ASEAN can also highlight best practices for ecosystem-wide intelligence sharing by developing guidelines that promote multi-sector collaboration. For example, Meta's Fraud Intelligence Reciprocal Exchange (FIRE) programme, piloted in Australia and now adopted in the UK, allows banks to share threat intelligence directly with the platform, resulting in the removal of nearly 30,000 scam advertisements and showcasing the impact of cross-industry cooperation.[30] ASEAN could consider regionalising such initiatives in consultation with stakeholders such as the ASEAN Banking Association and digital platforms operating in the region.

3. Regional Cooperation for Response and Recovery

Scam operations exploit uneven investigative capacity and gaps in cross-border coordination across the region. A dedicated regional enforcement mechanism to combat scams can institutionalise multilateral enforcement cooperation, enabling AMS to move towards more structured and consistent coordination. ASEANAPOL already coordinates the Working Group Meeting on Anti-Scam Operations, addressing scam centres. Building on this, a Regional Task Force on Digital Scams could be established in consultation with relevant bodies such as the ASEAN Ministerial Meeting on Transnational Crime.[31] The task force could undertake the following:

- **Promoting regional simulation exercises or coordination drills.** Drawing from existing cross-border trafficking investigation models, the task force can lead in designing drills and joint investigation exercises that focus on coordinated, cross-border enforcement. These efforts can be applied to stopping scam compounds and centres, while also improving the detection of human trafficking activities linked to scam syndicates. For example, the Regional Support Office of the Bali Process, an organisation focused on combatting human trafficking, has hosted workshops on online trafficking investigations and cross-border cooperation focused on scam centres.[32] These platforms can be expanded to incorporate scam-focused scenarios and shared enforcement techniques in the SEA context.

- **Pilot joint operations to test arrest coordination and asset recovery protocols.** ASEAN can build on successful models like Singapore's *FRONTIER+* initiative, launched in 2024 with Malaysia, Thailand, South Korea, Hong Kong SAR and the Maldives. Through structured multi-agency coordination, the initiative recovered over USD 88,000 in scam proceeds—demonstrating the operational impact of cross-border enforcement alliances.[33]

- **Standardise enforcement procedures through a regional playbook.** A shared manual aligned with the ASEAN Mutual Legal Assistance Treaty could provide guidance on evidence preservation, legal handovers, cross-border notification, and victim restitution.[34] Complementing this, ASEAN should promote a regional secondment and joint training programme where officers from AMS are embedded in peer agencies or within the task force itself. Focus areas could include cryptocurrency forensics, scam typology analysis, and maintaining a secure digital chain of custody.

4. Collaborative Innovation

Artificial intelligence (AI) and other technologies hold much potential for scam detection, triage, and recovery. The challenge however is to ensure that those solutions are properly tested and deployed in a coordinated, ethical and privacy-preserving manner. AMS can collaborate to make SEA the testbed and launchpad for AI solutions to detect, identify and respond to scams. Avenues to creating an enabling environment to test and scale new solutions include:

- **Ensuring alignment with ASEAN's digital governance frameworks**, including the *Guide on AI Governance and Ethics*,[35] *DEFA*, and existing regional cybersecurity strategies. These standards will safeguard transparency, inclusivity, and user trust in AI-enabled responses.

- **Developing a structured AI testing framework tailored to scams, supported by regional guidelines with clear evaluation metrics and benchmarks.** Such a framework would help ASEAN operationalise cutting-edge solutions, such as phishing classifiers, behavioural analytics, anomaly detection engines, and chatbot-enabled triage systems, while preserving trust, accelerating regional adoption, and enabling faster, data-driven

intervention. Singapore's AI Verify Framework, which provides a governance testing protocol to assess the responsible implementation of AI systems, can offer a useful reference. Alignment with broader regional digital governance frameworks would further support safe, scalable adoption. Without such coordination, AI efforts risk remaining fragmented and underutilised.

- **Creating testing environments for cross-border scam response,** such as a Regional AI Sandbox that allows solution providers to pilot, validate, and scale AI-powered tools, including anomaly detection and phishing classifiers, in a secure and collaborative setting. Sandbox corridors spanning two or more AMS would be anchored in standardised validation frameworks and agreed technical and regulatory protocols to support cross-border deployment and scalability.[36] This approach would foster policy learning, rapid adoption and iterative vetting as a **verified anti-scam tool.**

TECH FOR GOOD INSTITUTE

III. A Whole-of-ASEAN Approach against Scams

SEA has the potential to evolve from being a scam hotspot to becoming a model of cooperative scam management across dimensions, sectors and stakeholders. ASEAN is well-placed to facilitate this transition, but this effort requires a whole-of-community response across the ASEAN Political-Security Community, the ASEAN Economic Community, and the ASEAN Socio-Cultural Community.

First, **ASEAN and AMS can build on existing progress.** As highlighted throughout this report, ASEAN already has a strong foundation for regional coordination. Mechanisms such as the ASEAN Cybersecurity Coordinating Committee and the ASEAN network of national CERTs have laid the groundwork for technical cooperation.[37] Mechanisms such as the ASEAN Working Group on Anti-Online Scams, the ASEAN Senior Officials Meeting on Transnational Crime, and the ASEAN Working Group on Digital Economy provide important platforms for coordination. Financial, technical, and telecommunications integration efforts will also rely on bodies such as the ASEAN Instant Payments Working Group, the ASEAN Committee on Consumer Protection, and relevant regional platforms involving telecom regulators and service providers.

Through these groups, ASEAN can align emerging national mechanisms, such as scam response centres, with existing regional platforms. This approach will ensure that AMS can address threats in a timely, coordinated, and resource-efficient manner.

ASEAN is also advancing initiatives that will support regional anti-scam efforts. The ASEAN Unique Business Identification Number (UBIN), for example, will enable verification in business-to-business transactions, including for smaller companies.[38] Looking ahead, the DEFA presents a timely opportunity to promote interoperability of digital identity, advance shared telecom-level verification standards and encourage cooperation on digital trust. Similarly, the ASEAN Economic Community's Strategic Plan for ASEAN Vision 2045 highlights interoperable digital identity and authentication as a long-term priority.[39] Together, these initiatives demonstrate how scam management can be embedded within ASEAN's broader regional integration agenda, linking immediate progress with future pathways for resilience

Coordinating across **all three ASEAN Communities** requires a secretariat. For example, law enforcement coordination falls under the ASEAN Political-Security Community, digital trust and the digital economy under the ASEAN Economic Community, and community engagement and culturally sensitive messaging under the ASEAN Socio-Cultural Community. To navigate this complexity, **ASEAN and AMS can consider developing a strategic action plan for such coordination through the WG-AS** as the main coordinating body to streamline implementation and clarify roles and responsibilities across ASEAN.

While ASEAN aspires to regional integration, building resilience against digitally-enabled scams is not unlike other ASEAN efforts in which **a modular approach** can be adopted. Participation frameworks such as "ASEAN 2+X" or "ASEAN Minus X," could allow countries to pilot initiatives bilaterally or in small clusters before scaling them region-wide.[40] This phased approach allows AMS to innovate and align incrementally, without being constrained by the need for full consensus. It also respects national contexts while reinforcing shared regional objectives. Furthermore, these modular frameworks could also extend beyond ASEAN, reflecting its existing partnerships with dialogue and regional partners.

Last but not least, the rapidly evolving nature of scams necessitates regular review, assessment, and evidence-based evaluation of existing national and regional scam management capabilities can identify gaps, track emerging trends, and support adaptation. Regional think tanks and academic institutions can partner with WG-AS in this area, while platforms like the ATTS can host discussions around research, data, and analysis to make policy recommendations and improve implementation.

In summary, ASEAN can play an important role in **s**trengthening regional preparedness for coordinated scam management across the region. This effort will allow AMS to build on the digital momentum of the last decade, advance digital interoperability and trust, and support regional integration to realise the ASEAN 2045 Vision of building a “resilient, innovative, dynamic, and people-centred” ASEAN.

References

[1] ASEAN (2025b). Bangkok Digital Declaration. Retrieved 14 June 2025 from https://web.archive.org/web/20250630055145/https://asean.org/bangkok-digital-declaration/

[2] Cowling, M., et al. (2024). Untangling digital safety, literacy, and wellbeing in school activities for 10 to 13 year old students. *Education and Information Technologies,* 30(1), 941–958. Retrieved 15 August 2025 from https://doi.org/10.1007/s10639-024-13183-z

[3] Rogers, S. (2024, October 15). *New GASA report estimates $688 billion in scam losses across Asia amid rising cyberthreat worldwide.* Global Anti-Scam Alliance (GASA). Retrieved 15 August 2025 from https://web.archive.org/web/20250815023614/https://www.gasa.org/post/2024-asia-scam-report-688-billion-lost

[4] ASEAN (2020b). ASEAN Digital Masterplan 2025. Retrieved 14 June 2025 from https://web.archive.org/web/20250630055635/https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

[5] ASEAN. (2025b).

[6] ASEAN. (2025d).

[7] FCC (2019). Combating Spoofed Robocalls with Caller ID Authentication. Retrieved 14 June 2025 from https://web.archive.org/web/20250610050155/https://www.fcc.gov/call-authentication

[8] Lekab (2025). RCS - better protection against fraud. Retrieved 14 June 2025 from https://web.archive.org/web/20250407234907/https://www.lekab.com/en/insights/rcs-better-protection-against-fraud

[9] Mastercard (2023). Mastercard leverages its AI capabilities to fight real-time payment scams. Retrieved 17 September 2025 from https://www.mastercard.com/news/europe/en-uk/newsroom/press-releases/en-gb/2023/mastercard-leverages-its-ai-capabilities-to-fight-real-time-payment-scams/

[10] Digital News Asia (2023, August 14). Singtel partners AIS and Maxis to fight rising digital scams. Digital News Asia. Retrieved 22 September 2025 from https://www.digitalnewsasia.com/business/singtel-partners-ais-and-maxis-fight-rising-digital-scams

[11] Buchanan, R., & Ulrich, L. (2002). U.S. cybersecurity: A family of policies for the 21st century. J*ournal of Homeland Security and Emergency Management,* 1(3). Retrieved 14 June 2025 from https://doi.org/10.3390/ijerph22060938

[12] Rogers, S. (2024, September 25). *37 billion reasons the citizens of Malaysia, Thailand, and Taiwan need better scam protection.* Global Anti-Scam Alliance (GASA). Retrieved 14 June 2025 from https://web.archive.org/web/20250702155354/https://www.gasa.org/post/where-did-the-billions-go-in-malaysia-thailand-taiwan

[13] Ibid.

[14] Okeleke, K. (2025). Towards a digital nation: Addressing the scam economy in Asia Pacific. GSMA Intelligence. Retrieved 14 June 2025 from https://web.archive.org/web/20250702155503/https://www.gsma.com/about-us/regions/asia-pacific/wp-content/uploads/2025/03/240325-Towards-a-digital-nation.pdf

[15] ScamShield. (n.d.). Avenues of support. Retrieved 14 June 2025 from https://web.archive.org/web/20250702162454/https://www.scamshield.gov.sg/avenues-of-support/

[16] Weaver, J., & O'Connor, S. (2023). Cultivating Coordination. ANU Tech Policy Design Centre. Retrieved 14 June 2025 from https://web.archive.org/web/20250702041120/https://techpolicy.au/wp-content/uploads/2023/08/Web_TPDC_Cultivating-Coordination_NO.2_Feb-2023.pdf

[17] ASEAN (2025d). ASEAN Guideline on the Implementation of the Non-Punishment Principle for Protection of Victims of Trafficking in Persons. Retrieved 14 June 2025 from https://web.archive.org/web/20250702161943/https://asean.org/wp-content/uploads/2025/06/ASEAN-Guideline-on-the-Implementation-of-the-Non-Punishement-Principle-for-Protection-of-Victims-of-Trafficking-in-Persons-adopted-ad-referendum-on-27-May-2025.pdf

[18] World Economic Forum. (n.d.). Cybersecurity Learning Hub. Retrieved 14 June 2025 from https://web.archive.org/web/20250702034756/https://www.weforum.org/projects/cybersecurity-learning-hub/

[19] Tortermvasana, K. (2025). Biometric SIM card registration approved. *Bangkok Post*. Retrieved 14 June 2025 from https://web.archive.org/web/20250330153728/https://www.bangkokpost.com/business/general/2945410/biometric-sim-card-registration-approved

[20] Infocomm Media Development Authority (IMDA) (n.d.). Anti-Scam Measures. Retrieved 14 June 2025 from https://web.archive.org/web/20250702154716/https://www.imda.gov.sg/how-we-can-help/anti-scam-measures

[21] Cyber Security Agency of Singapore (2021). ASEAN-Singapore Cybersecurity Centre of Excellence. Retrieved 14 June 2025 from https://web.archive.org/web/20250520225331/https://www.csa.gov.sg/news-events/press-releases/asean-singapore-cybersecurity-centre-of-excellence

[22] ASEAN-Japan Cybersecurity Capacity Building Centre (2017). About Us. Retrieved 14 June 2025 from https://web.archive.org/web/20250117102155/https://ajccbc.ncsa.or.th/about-us/

[23] ASEAN-Japan Cybersecurity Capacity Building Centre (2024). Cyber SEA Game 2024. Retrieved 14 June 2025 from https://web.archive.org/web/20250512114644/https://ajccbc.ncsa.or.th/rules/

[24] Singapore Police Force (2024). Mid-Year Scams and Cybercrime Brief 2024 Total Scam and Cybercrime Cases. Retrieved 14 June 2025 from https://web.archive.org/web/20250322001031/https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2024_mid_year_scams_and_cybercrime_brief.pdf

[25] Binh, T. (2024). NCA releases a new app to combat online fraud in Vietnam. SGGP English Edition. Retrieved 14 June 2025 from https://web.archive.org/web/20240801041810/https://en.sggp.org.vn/nca-releases-new-app-to-combat-online-fraud-in-vietnam-post111526.html

[26] Detros, K. (2025). Towards human-centric approaches to cyber resilience in Southeast Asia. Tech For Good Institute. Retrieved 14 June 2025 from https://web.archive.org/web/20250702155715/https://techforgoodinstitute.org/blog/expert-opinion/towards-human-centric-approaches-to-cyber-resilience-in-southeast-asia/

[27] Singapore Police Force (2022). Opening of Anti-Scam Command Office. Retrieved 14 June 2025 from https://web.archive.org/web/20250610140910/https://www.police.gov.sg/Media-Room/News/20220906_opening_of_anti-scam_command_office

[28] ASEAN (2021a). ASEAN Data Management Framework. Retrieved 14 June 2025 from https://web.archive.org/web/20250702035547/https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf

[29] DNS Research Federation (2025). Microsoft, Meta and others join the Global Signal Exchange (GSE). Retrieved 14 June 2025 from https://web.archive.org/web/20250422215600/https://dnsrf.org/blog/microsoft--meta-and-others-join-the-global-signal-exchange--gse-/index.html

[30] Cybernews (2024). Meta's FIRE pulls thousands of 'celeb bait' scam ads off Facebook, Instagram. Retrieved 17 September 2025 from https://cybernews.com/security/meta-fire-celeb-bait-scam-ads-facebook-instagram-uk-australia-banks/

[31] ASEAN. (2023, September 19). ASEAN Ministerial Meeting on Transnational Crime (AMMTC). ASEAN. Retrieved 14 June 2025 from https://web.archive.org/web/20250702161628/https://asean.org/asean-ministerial-meeting-on-transnational-crime-ammtc/

[32] Regional Support Office of the Bali Process. (2025, February 20). Technical Workshop: Building Online Investigations Capacity to Address Trafficking in Persons into Cyber-Scam Centres and Related Transnational Crime. Retrieved 14 June 2025 from https://web.archive.org/web/20250702162021/https://rso.baliprocess.net/calendar/technical-workshop-building-online-investigations-capacity-to-address-trafficking-in-persons-into-cyber-scam-centres-and-related-transnational-crime-2/

[33] ScamShield (2025). Annual Scams and Cybercrime Brief 2024: Overall Scams and Cybercrime Situation in 2024. Retrieved 14 June 2025 from https://web.archive.org/web/20250630081213/https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2024_annual_scams_and_cybercrime_brief.pdf

[34] ASEAN (n.d.). Treaty on Mutual Legal Assistance in Criminal Matters. Retrieved 14 June 2025 from https://web.archive.org/web/20250630081004/https://asean.org/our-communities/asean-political-security-community/rules-based-people-oriented-people-centred/treaty-on-mutual-legal-assistance-in-criminal-matters/

[35] ASEAN (2024). ASEAN Guide on AI Governance and Ethics Contents. Retrieved 14 June 2025 from https://web.archive.org/web/20250630081551/https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf

[36] Tech For Good Institute. (2025). Sandbox to Society: Fostering innovation in Southeast Asia. Retrieved 14 June 2025 from https://web.archive.org/web/20250702162244/https://techforgoodinstitute.org/research/tfgi-reports/sandbox-to-society-fostering-innovation-in-southeast-asia/

[37] ASEAN (2021b). ASEAN Cybersecurity Cooperation Strategy. Retrieved 14 June 2025 from https://web.archive.org/web/20250609110248/https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

[38] ASEAN (2025c). Implementation Roadmap to Establish Regionally Comparable and Recognised UBIN in ASEAN. Retrieved 14 June 2025 from https://web.archive.org/web/20250702154916/https://asean.org/wp-content/uploads/2025/04/Public-Summary-of-Implementation-Roadmap-to-Establish-Regionally-Comparable-and-Recognised-UBIN-in-ASEAN-1.pdf

[39] ASEAN. (2025a). ASEAN 2045: Our shared future (Section 3.1.5). Retrieved 15 August 2025 from https://web.archive.org/web/20250815025227/https://asean.org/wp-content/uploads/2025/05/ASEAN-2045-Our-Shared-Future.pdf

[40] Ng, J. (2021). Extending the 'ASEAN Minus X' Formula. In Contesting Sovereignty: Power and Practice in Africa and Southeast Asia (pp. 224–252). Cambridge: Cambridge University Press. Retrieved 14 June 2025 from https://doi.org/10.1017/9781108854320.012

Annex I: Supporting National Capacity

	Potential Model	Tech	People	Institutions	Policy
Facilitating knowledge exchange	ASEAN Cybersecurity Capacity Building Programme,	Regional digital knowledge & learning hub (platform) consolidating toolkits, case studies, after-action reports	ASEAN Scam Awareness Network	Regional public-private knowledge and learning hub (governance/hosting)	Facilitating sharing of best practices and implementation challenges around relevant laws, such as payments, cybercrime and consumer protection
Setting regional standards, protocols or principles for interoperability	ASEAN Taxonomy for Sustainable Finance	SIM registration, regulating messaging platforms and supporting digital identity interoperability for cross-border verification. Standardised caller/business verification protocols (e.g., STIR/SHAKEN, RCS Business Messaging) and consumer notice templates		Shared scam taxonomy	Minimum reporting schema aligned with the ASEAN Data Management Framework; model data-sharing agreements; privacy/data-protection alignment

	Potential Model	Tech	People	Institutions	Policy
Developing resources and toolkits	Model Contractual Clauses, Guidelines	Catalogue of verified anti-scam tools	Repository of community engagement models	Document models of inter-agency coordination Toolkit for national anti-scam coordination units Standardised training resources, hosting cross-border case workshops, and monitoring implementation	Implementation guides for the non-punishment principle; victim-redress standards; notice-and-takedown SOPs; legal templates for freezing funds and preserving evidence
Facilitating technical assistance	ASCCE & AJCCBC as anchors; ASEANAPOL / WC-PSS clinics; regional helpdesk/peer-review mechanism	Expert missions & embedded advisors; reference implementations and sandboxes (AI/identity/caller-ID); federated-learning pilots; interoperability testing	Victim support training programme for frontline responders	Regional training framework for scam detection and response Practices for information sharing, roles and responsibilities, escalation pathways and decision-making procedures	Sandbox-design support; peer-to-peer regulatory mentoring; adoption support for model alignment